Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Monitor and Troubleshoot Across Cloud and Hybrid IT to Minimize Alert Storms

OBS1338C

Aaron Kirk

Principal Product Manager | Splunk

Yaroslav Tytar

Product Manager | Splunk

splunk> .conf22

Aaron Kirk

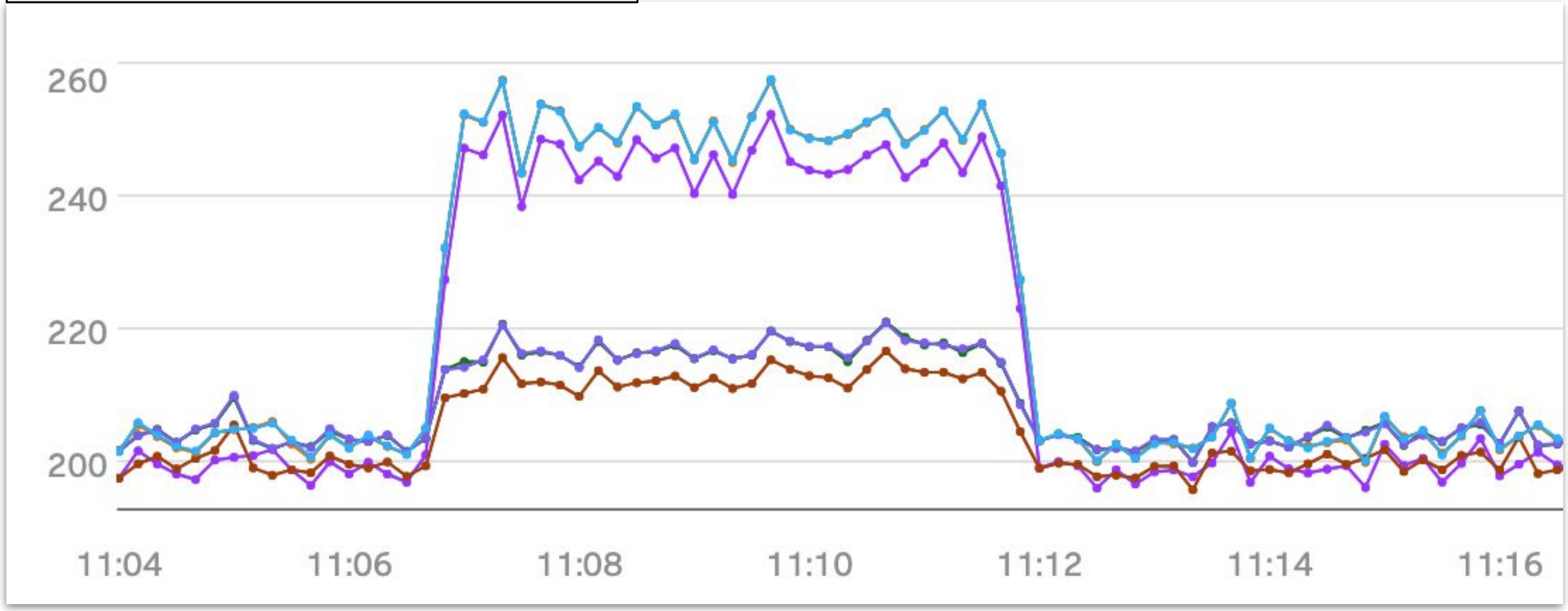
Principal PM | Splunk

Yaroslav Tytar

PM | Splunk

4 Unique Metric Time Series (MTS)

Metric Name: transaction_latency

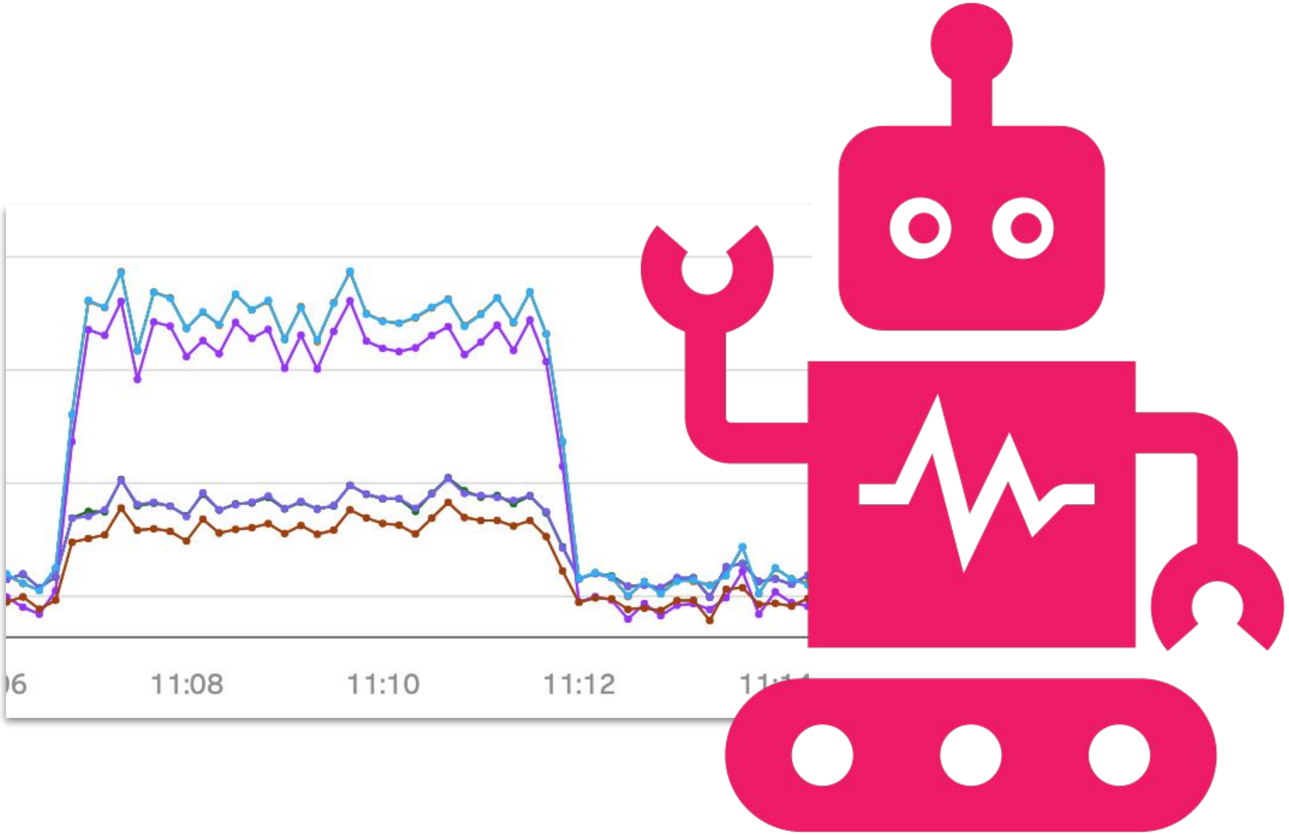


```
{
  “customer_name”: “Sleeping Beans”,
  “datacenter”: “The Moon”
}
```

```
{
  “customer_name”: “Sleeping Beans”,
  “datacenter”: “The Earth”
}
```

What is a Detector?

Your personal robot to assist with Observability



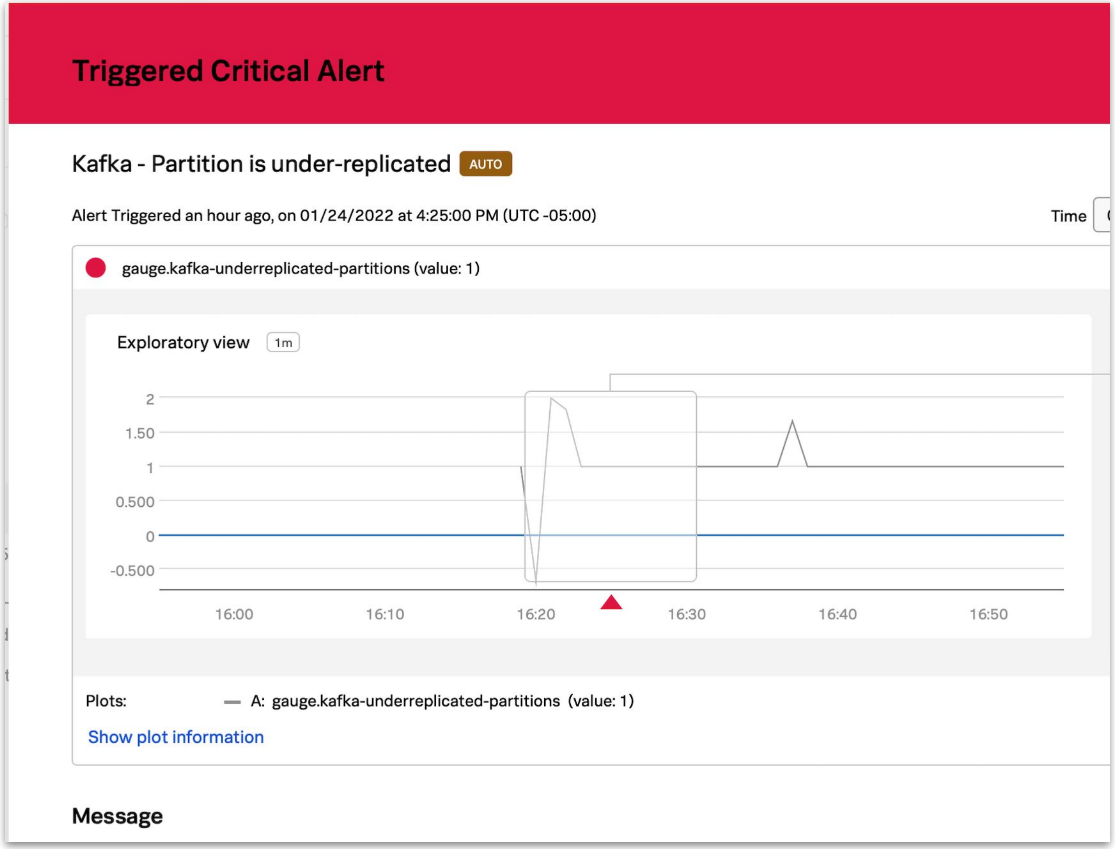
- Review data as it is received in the Splunk® Observability Cloud
- Decide when to alert using simple static thresholds or intelligent analytics
- Connects to outbound integration to send notifications or kickstart automation
- Super speedy!

End-to-End Workflow

1. Getting Data In (GDI)
2. Out-of-the-box Dashboards and Detectors (AutoDetect)
3. Custom Dashboards and Detectors

… Detectors constantly evaluating new data…

4. Alerts on Dashboards
5. Integrations - notifications and webhooks
6. Clearing Alerts



Triggered Critical Alert

Kafka - Partition is under-replicated AUTO

Alert Triggered an hour ago, on 01/24/2022 at 4:25:00 PM (UTC -05:00)

● gauge.kafka-underreplicated-partitions (value: 1)

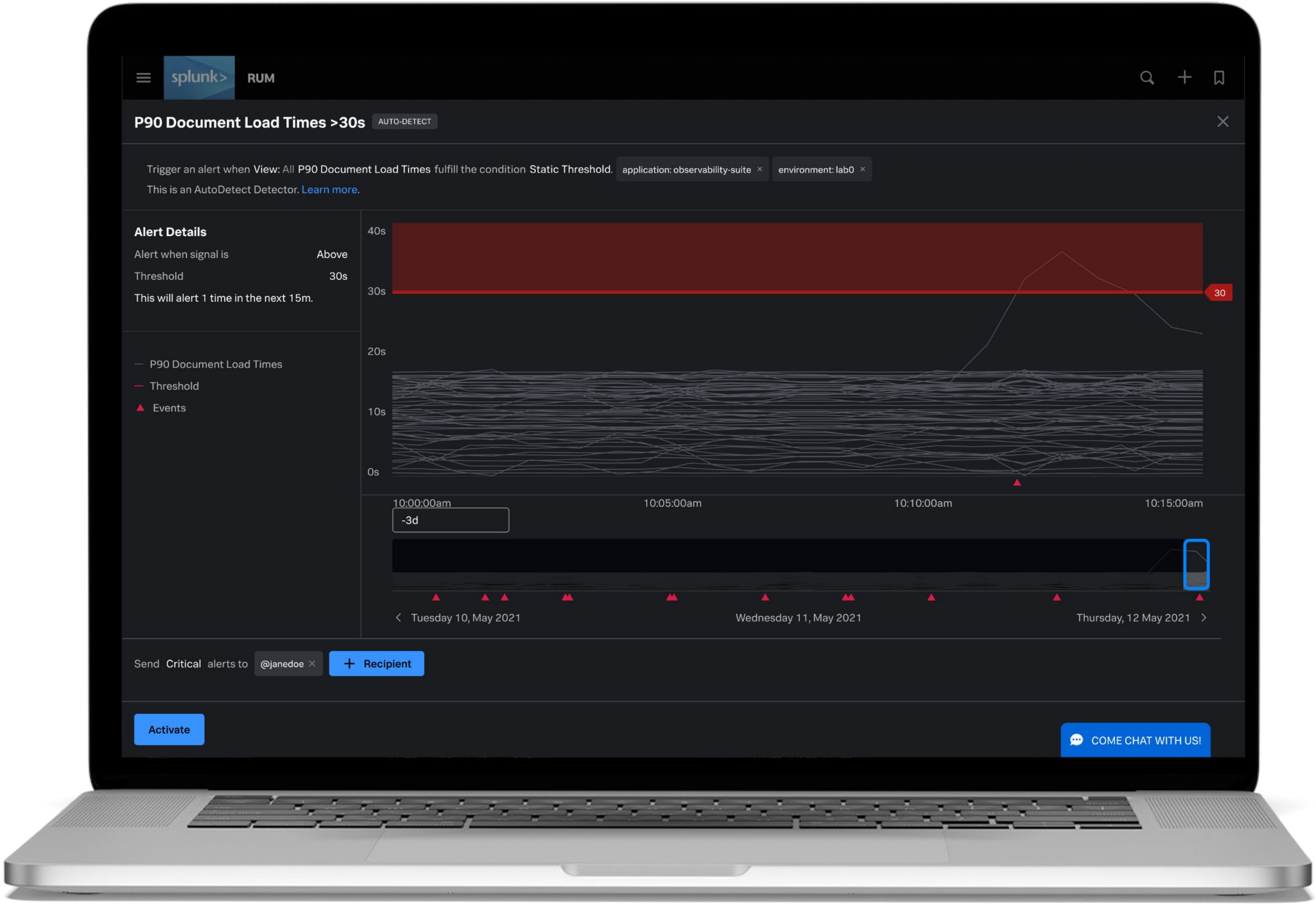
Plots: A: gauge.kafka-underreplicated-partitions (value: 1)

Message

AutoDetect

Simplified onboarding with out-of-the-box alerting

- **Faster TTV with OOTB problem detection** for critical components
- Automatically discover anomalies in your infrastructure
- Quickly identify infrastructure state with intuitive alert integration for **faster MTTR**



P90 Document Load Times >30s

Trigger an alert when View: All P90 Document Load Times fulfill the condition Static Threshold. application: observability-suite × environment: lab0 ×

This is an AutoDetect Detector. Learn more.

Alert Details

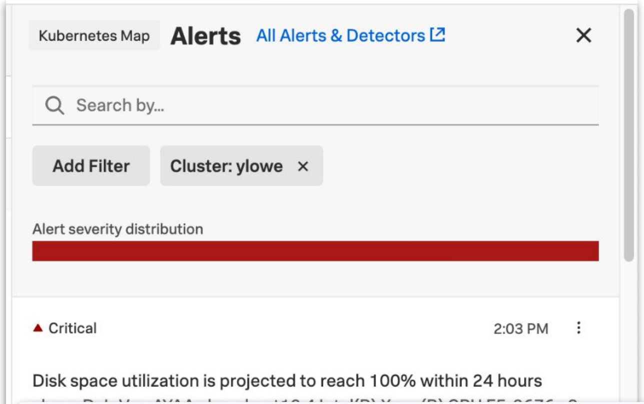
Alert when signal is	Above
Threshold	30s

This will alert 1 time in the next 15m.

Send Critical alerts to @janedoe ×

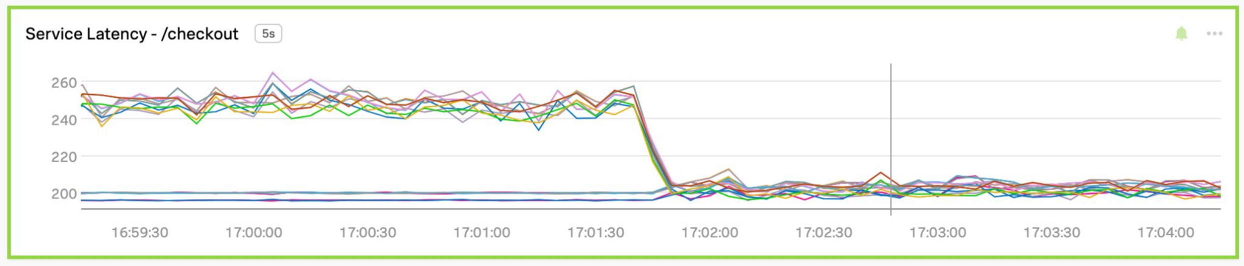
Alerts in Observability

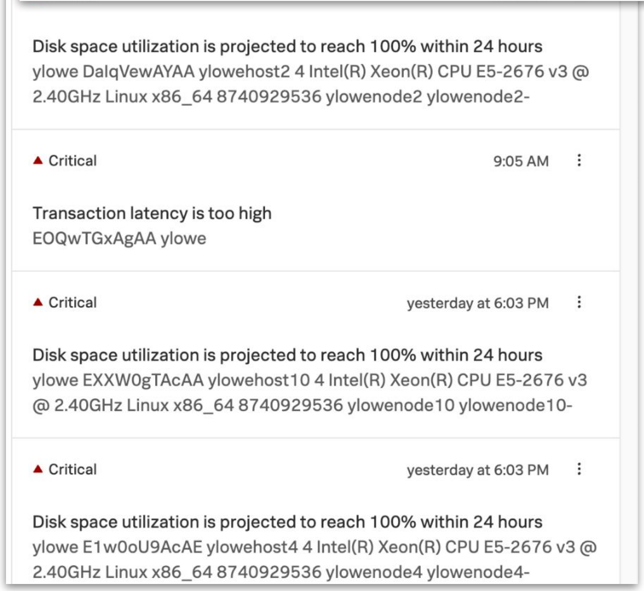
- View, search, and filter all alerts in a dedicated page
- Show related alerts in the alert sidebar
- Connect alerts to dashboards for simple in-context troubleshooting



Critical 2:03 PM

Disk space utilization is projected to reach 100% within 24 hours


Service Latency - /checkout 5s


Disk space utilization is projected to reach 100% within 24 hours
ylowe DalqVewAYAA ylowehost2 4 Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz Linux x86_64 8740929536 ylowenode2 ylowenode2-

Critical 9:05 AM

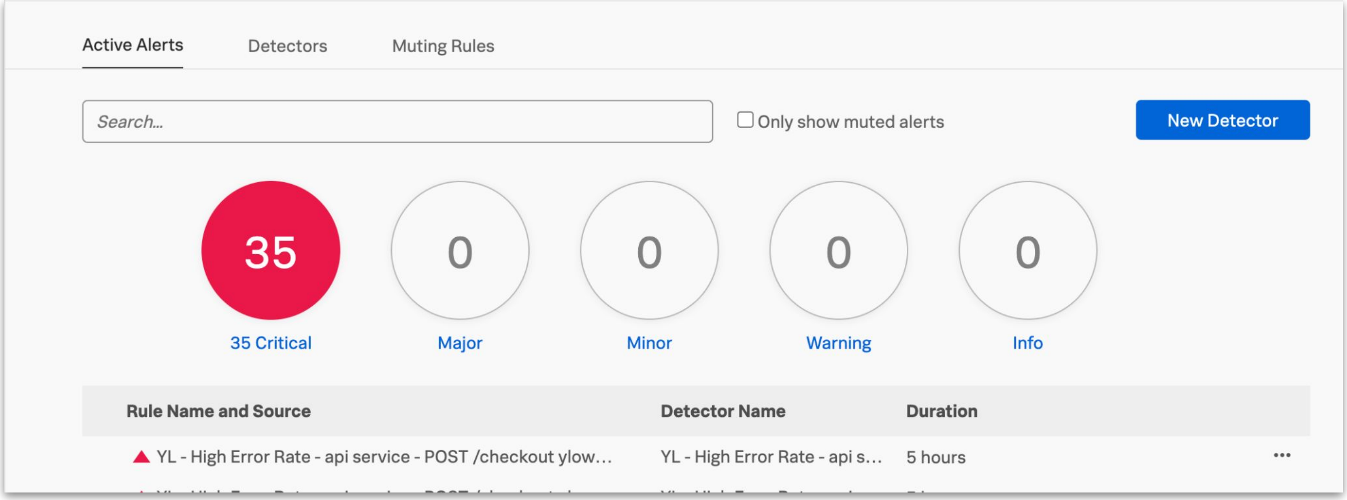
Transaction latency is too high
EOQwTGxAgAA ylowe

Critical yesterday at 6:03 PM

Disk space utilization is projected to reach 100% within 24 hours
ylowe EXXW0gTAcAA ylowehost10 4 Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz Linux x86_64 8740929536 ylowenode10 ylowenode10-

Critical yesterday at 6:03 PM

Disk space utilization is projected to reach 100% within 24 hours
ylowe E1w0oU9AcAE ylowehost4 4 Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz Linux x86_64 8740929536 ylowenode4 ylowenode4-



35	0	0	0	0
35 Critical	Major	Minor	Warning	Info

Rule Name and Source	Detector Name	Duration
YL - High Error Rate - api service - POST /checkout ylow...	YL - High Error Rate - api s...	5 hours

splunk> .conf22

Outbound Integrations

Connecting Observability to external services

Splunk On-Call

Slack

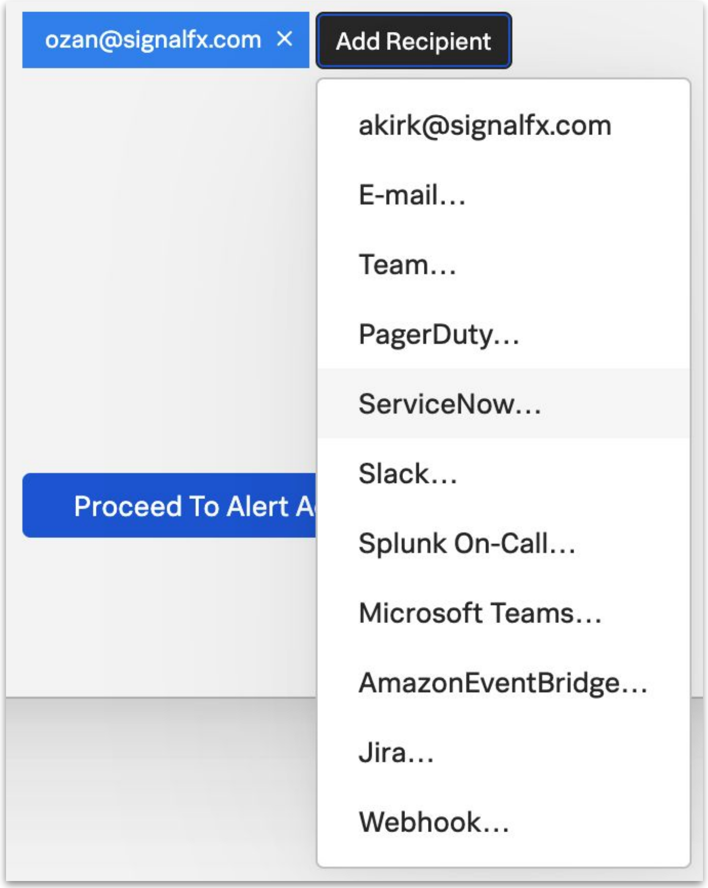
ServiceNow

PagerDuty

Jira

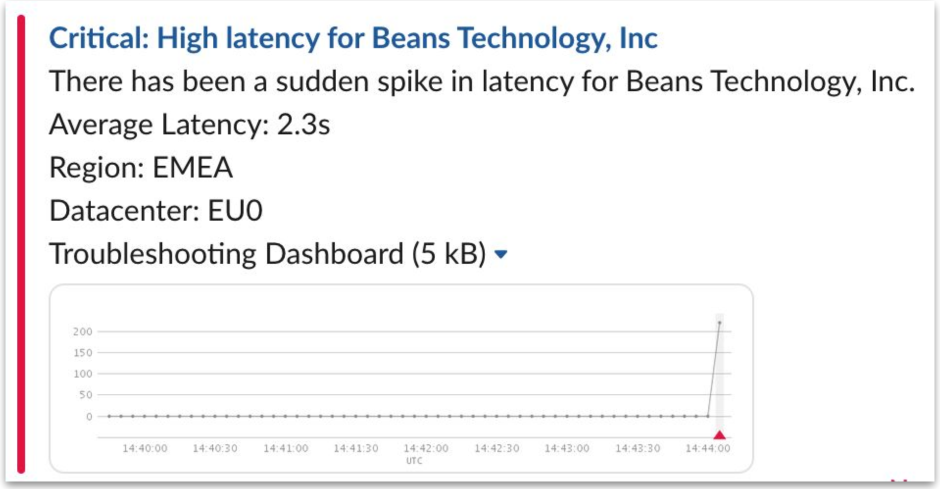
Custom Webhook

+ More



Customize the integration to pass vital context into downstream tools

Customizing the alert message and title



Critical: High latency for Beans Technology, Inc

There has been a sudden spike in latency for Beans Technology, Inc.

Average Latency: 2.3s

Region: EMEA

Datacenter: EU0

Troubleshooting Dashboard (5 kB) ▾

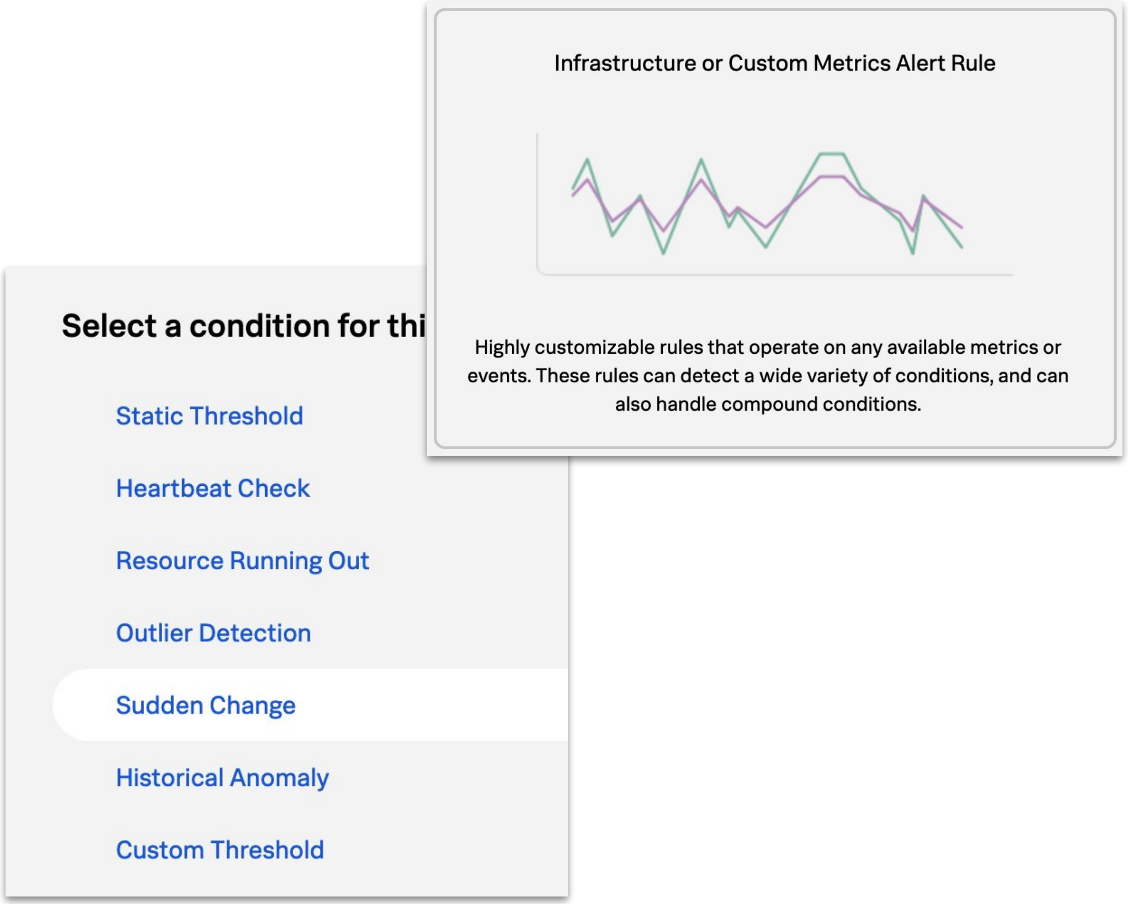
Detectors Across Observability

Infrastructure Monitoring and Custom Metrics

Get exactly the right signal

- select data
- define formulas
- aggregate data
- transform signals

Configure alert conditions with static thresholds or select an intelligent analytics-driven algorithm

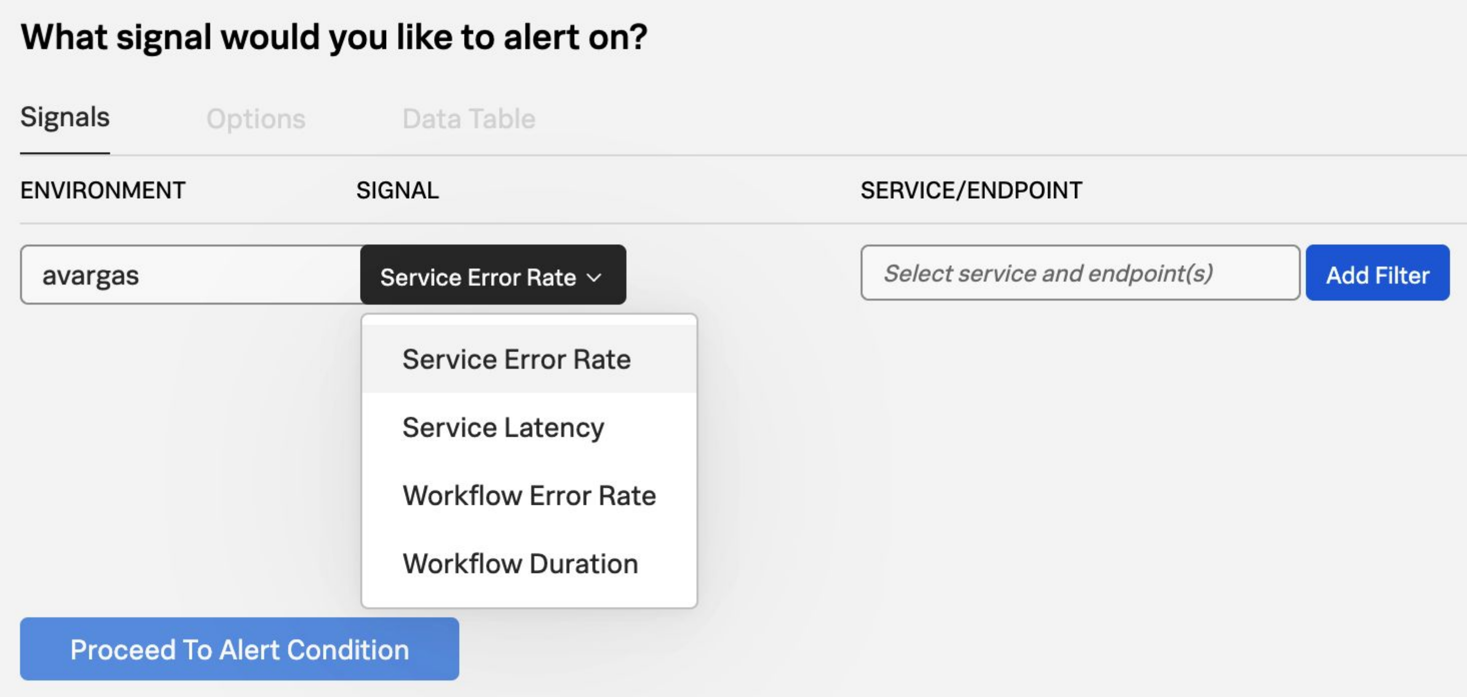


Infrastructure or Custom Metrics Alert Rule

Highly customizable rules that operate on any available metrics or events. These rules can detect a wide variety of conditions, and can also handle compound conditions.

Detectors Across Observability

APM

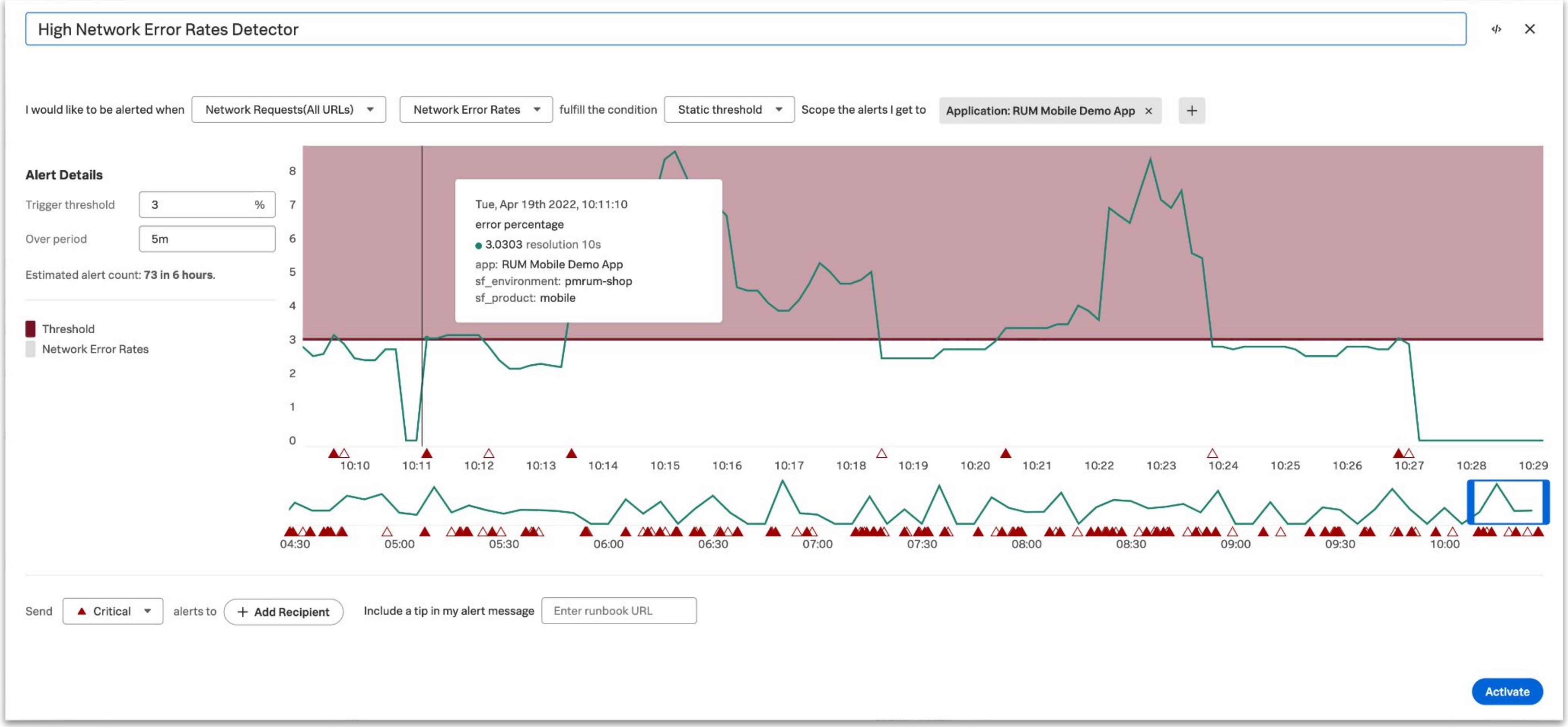


What signal would you like to alert on?

- Monitor error rate and latency for your Services and Business Workflows
- Identify sudden spikes and historical anomalies for a clear indication of changes

Detectors Across Observability

Real User Monitoring and Synthetics



High Network Error Rates Detector

I would like to be alerted when Network Requests(All URLs) ▾ Network Error Rates ▾ fulfill the condition Static threshold ▾ Scope the alerts I get to Application: RUM Mobile Demo App × +

Alert Details

Trigger threshold: 3 %

Over period: 5m

Estimated alert count: **73 in 6 hours.**

🟥 Threshold

▨ Network Error Rates

Tue, Apr 19th 2022, 10:11:10
error percentage
● 3.0303 resolution 10s
app: RUM Mobile Demo App
sf_environment: pmrum-shop
sf_product: mobile

Send ▲ Critical ▾ alerts to + Add Recipient Include a tip in my alert message Enter runbook URL

Activate

Best Practices for Alerting

Industry standards to ensure you alert on the things that matter

Understand your goal

Monitor symptoms of problems

Keep it simple

Include context & next steps

Be a Detector Jedi Master

Best practices to prevent alert storms and generate the right alerts at the right time.

splunk> .conf22

The Path to be a Detector Jedi Master

1

Understand the Force

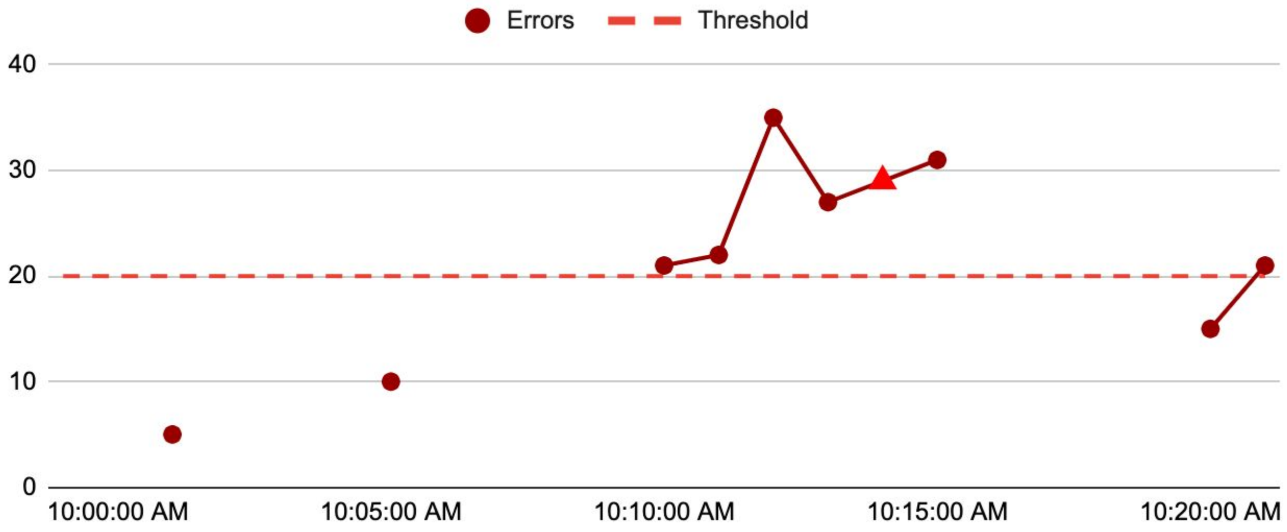
Understand your data
(Resolution, Periodicity,
Metadata, Aggregation)

Alerting with event-driven data

Best Practices in Data Selection - Aperiodic Data

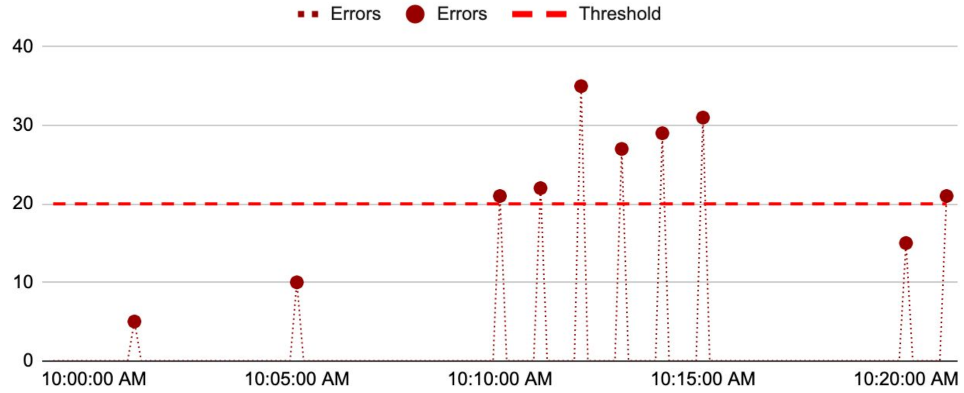
Data is sent on 1 minute interval, but only when errors occur

“Alert me when number of errors is above 20 for 5 min”



High chance alert would never be triggered!!!

Why? Because there is not enough data to determine correct resolution of the reporting metric.



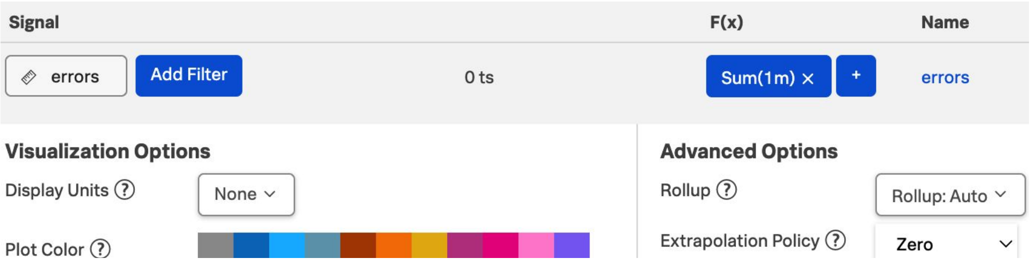
If resolution determined as lower than 1m (e.g. 10s) - there is not enough data points to trigger an alert

Alerting with event-driven data

Best Practices in Data Selection - Aperiodic Data

UI Solution

Sum over + Zero extrapolation policy



Signal: errors — Add Filter — 0 ts

F(x): Sum(1m) × — +

Name: errors

Visualization Options

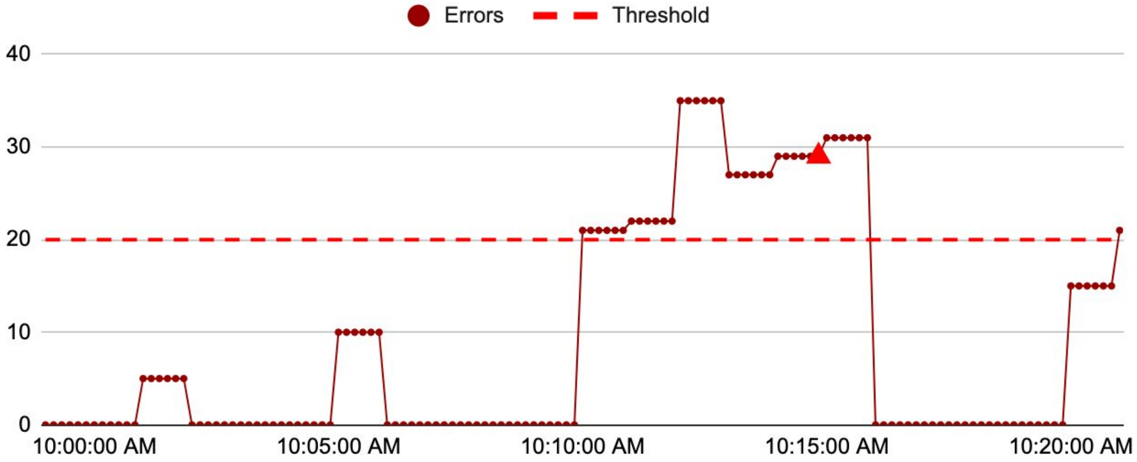
Display Units ⓘ: None

Plot Color ⓘ

Advanced Options

Rollup ⓘ: Rollup: Auto

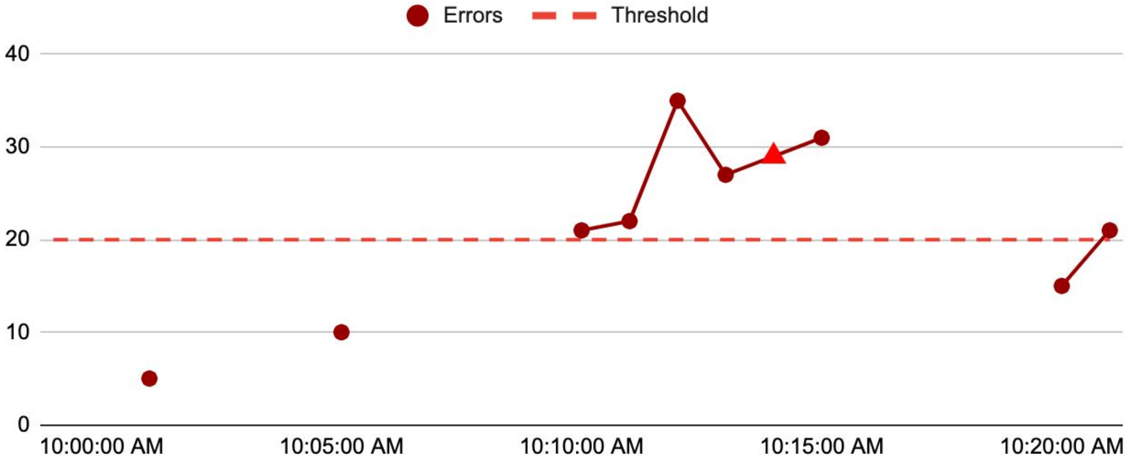
Extrapolation Policy ⓘ: Zero



SignalFlow Solution

specify resolution in your data block

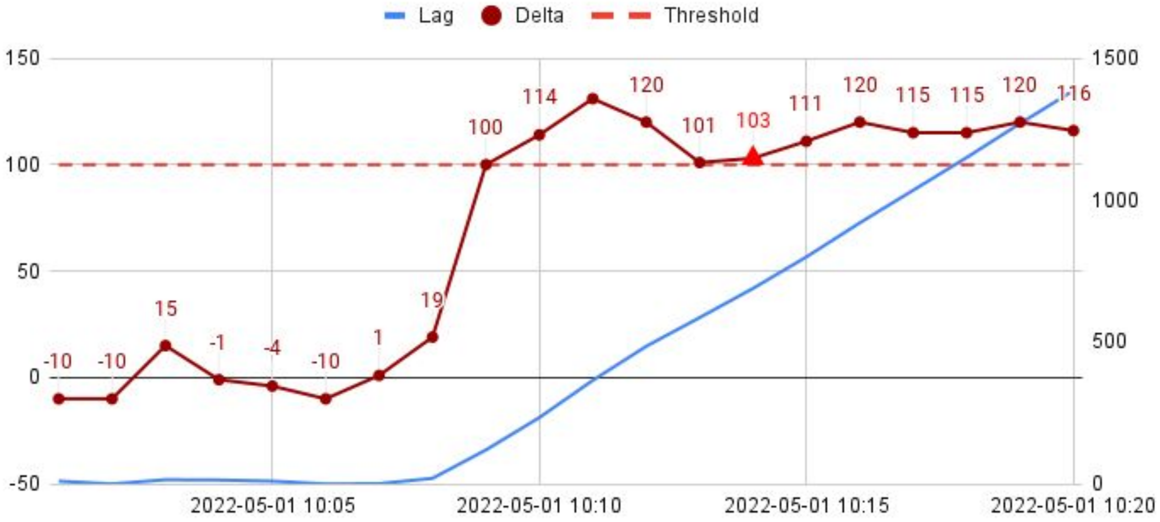
```
A = data('errors', resolution=60000).publish('A')
```



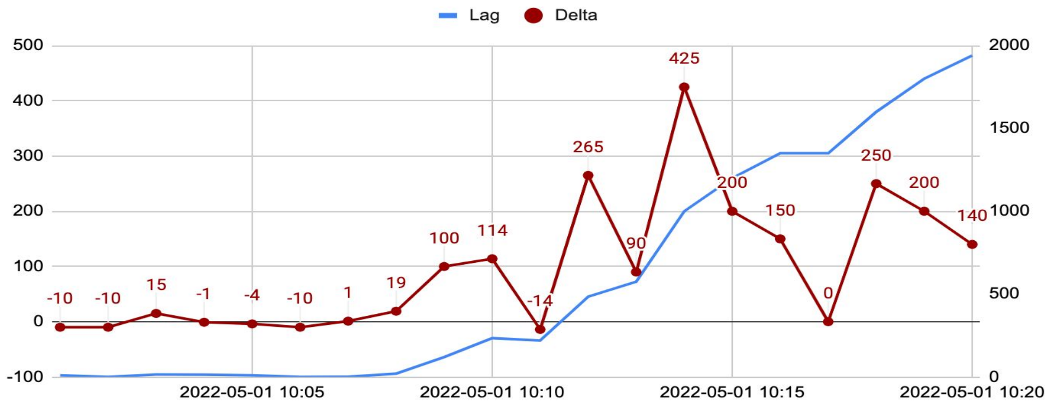
Challenge the scope

Best Practices in Data Selection

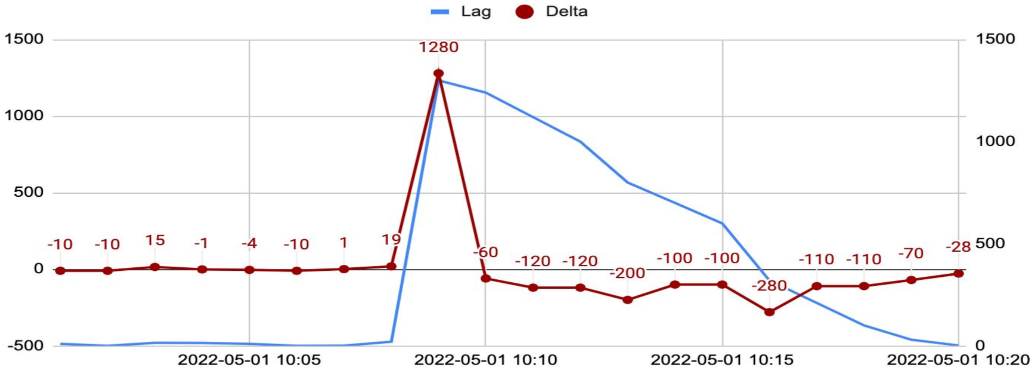
“Alert me when my kafka consumer lag is growing at least by 100 for 5 minutes”



Do I need to be alerted when the rate of growth is irregular

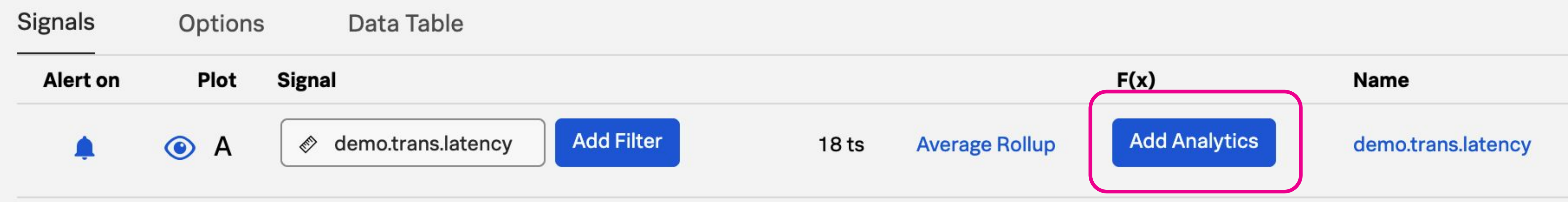


Do I need to be alerted on one-time spike



Aggregate with intention

Best Practices in Data Selection



Alert on	Plot	Signal				F(x)	Name
🔔	👁 A	demo.trans.latency	Add Filter	18 ts	Average Rollup	Add Analytics	demo.trans.latency

Demo metric demo.trans.latency with these dimensions:

demo_host
demo_customer
demo_datacenter

Fire an alert when the average latency of all hosts is above <value>

Fire an alert when the average latency for a particular customer is above <value>

The Path to be a Detector Jedi Master

1

2

Understand the Force

Understand your data (Resolution, Periodicity, Metadata, Aggregation)

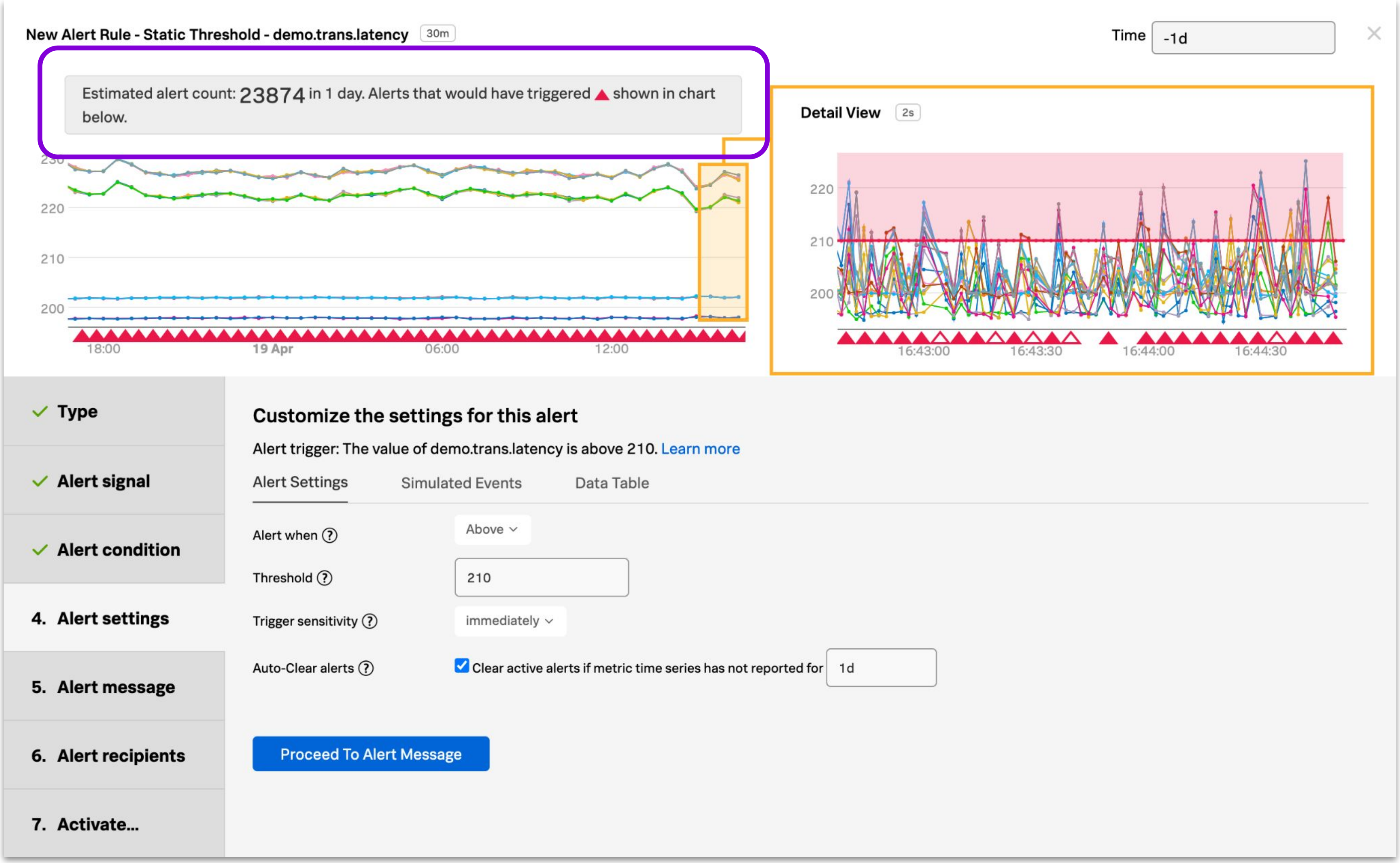
Use all available tools

Use functions available to create the right alerts (Rollup, Alert preview, trigger sensitivity, off conditions)

Alert Preview

Estimate how many alerts this detector configuration will create based on historical data.

Will update whenever you change the alert settings.



New Alert Rule - Static Threshold - demo.trans.latency 30m

Time -1d

Estimated alert count: 23874 in 1 day. Alerts that would have triggered ▲ shown in chart below.

Customize the settings for this alert

Alert trigger: The value of demo.trans.latency is above 210. Learn more

Alert when ⓘ Above

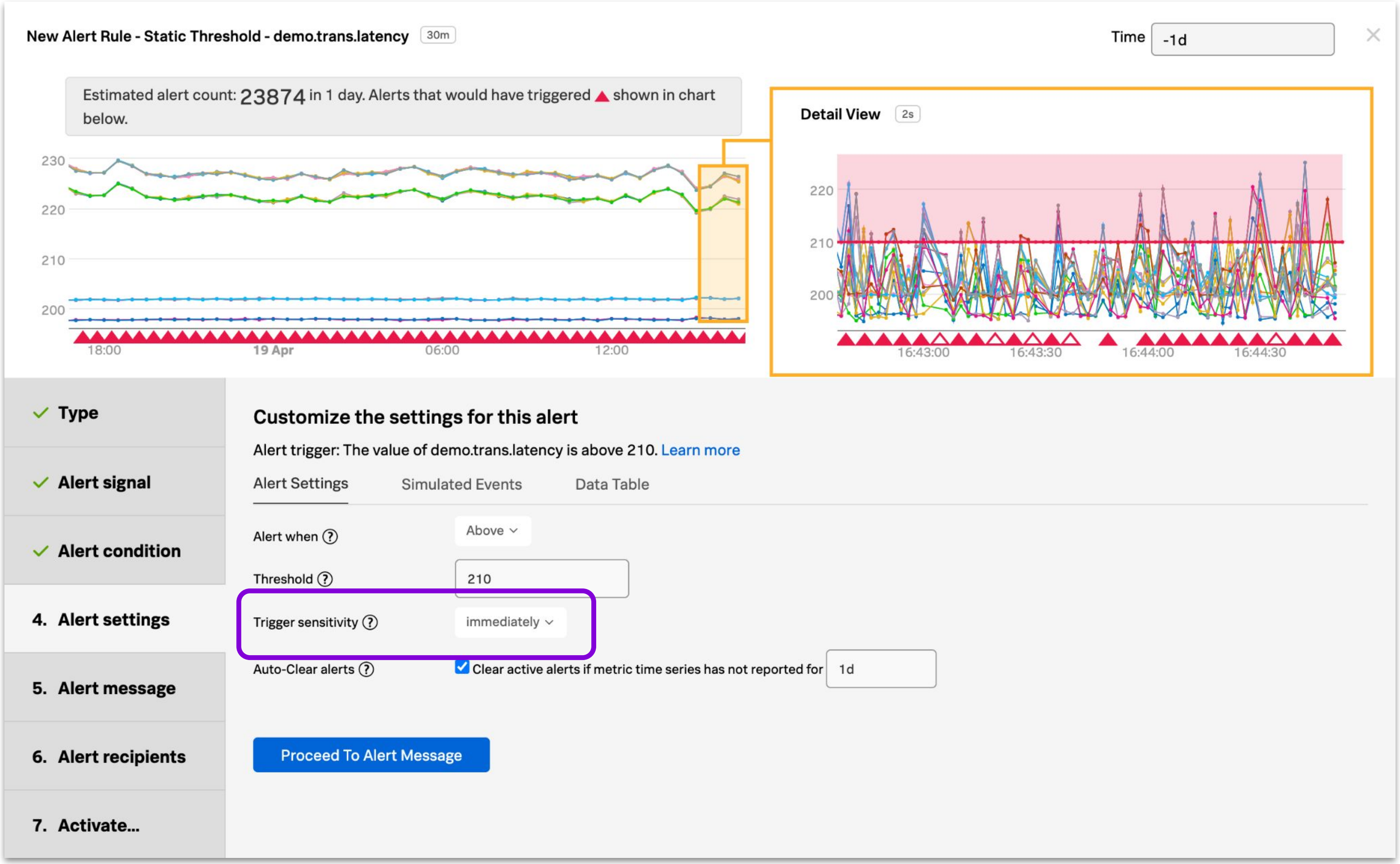
Threshold ⓘ 210

Trigger sensitivity ⓘ immediately

Auto-Clear alerts ⓘ ☑ Clear active alerts if metric time series has not reported for 1d

Trigger Sensitivity or “Lasting”

Reduce alert noise using ‘Trigger Sensitivity’



New Alert Rule - Static Threshold - demo.trans.latency 30m

Time -1d

Estimated alert count: 23874 in 1 day. Alerts that would have triggered ▲ shown in chart below.

✓ Type

✓ Alert signal

✓ Alert condition

4. Alert settings

5. Alert message

6. Alert recipients

7. Activate...

Customize the settings for this alert

Alert trigger: The value of demo.trans.latency is above 210. Learn more

Alert Settings | Simulated Events | Data Table

Alert when ⓘ: Above

Threshold ⓘ: 210

Trigger sensitivity ⓘ: immediately

Auto-Clear alerts ⓘ: ☑ Clear active alerts if metric time series has not reported for 1d

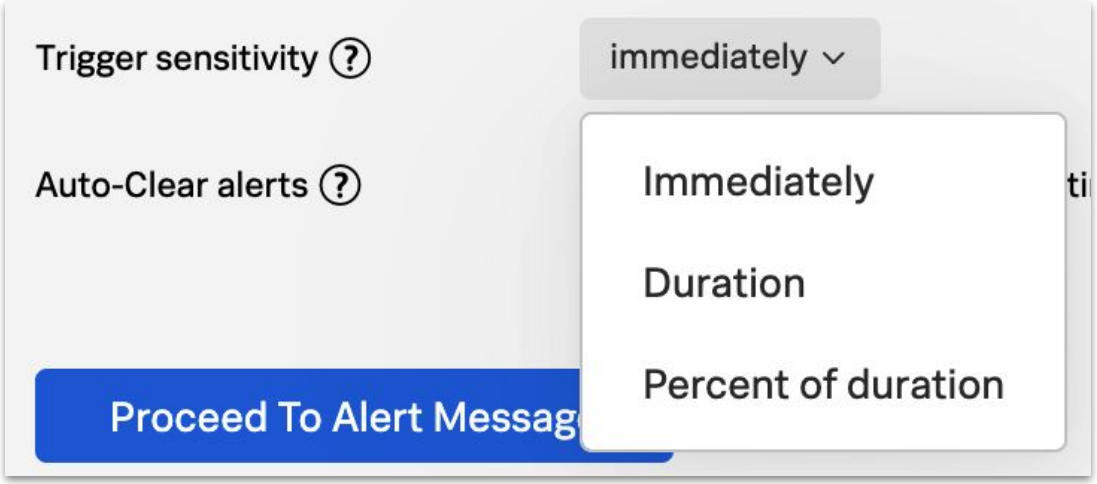
Proceed To Alert Message

Trigger Sensitivity or “Lasting”

Immediately - Fire alert when signal crosses the threshold

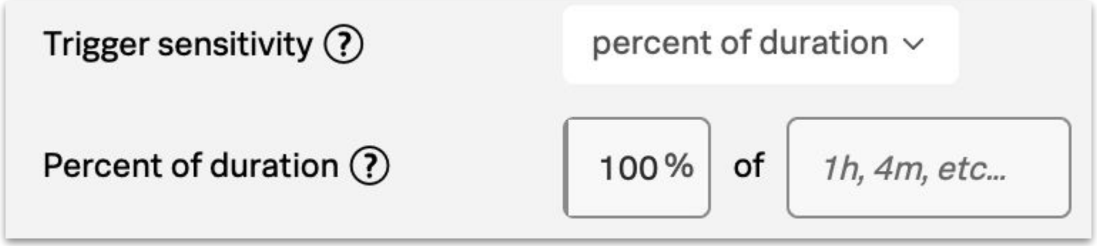
Duration - Fire alert when signal stays above threshold for <time>

Percent of duration - Fire alert when signal stays above threshold for <percent> of <time>



Trigger sensitivity ? immediately

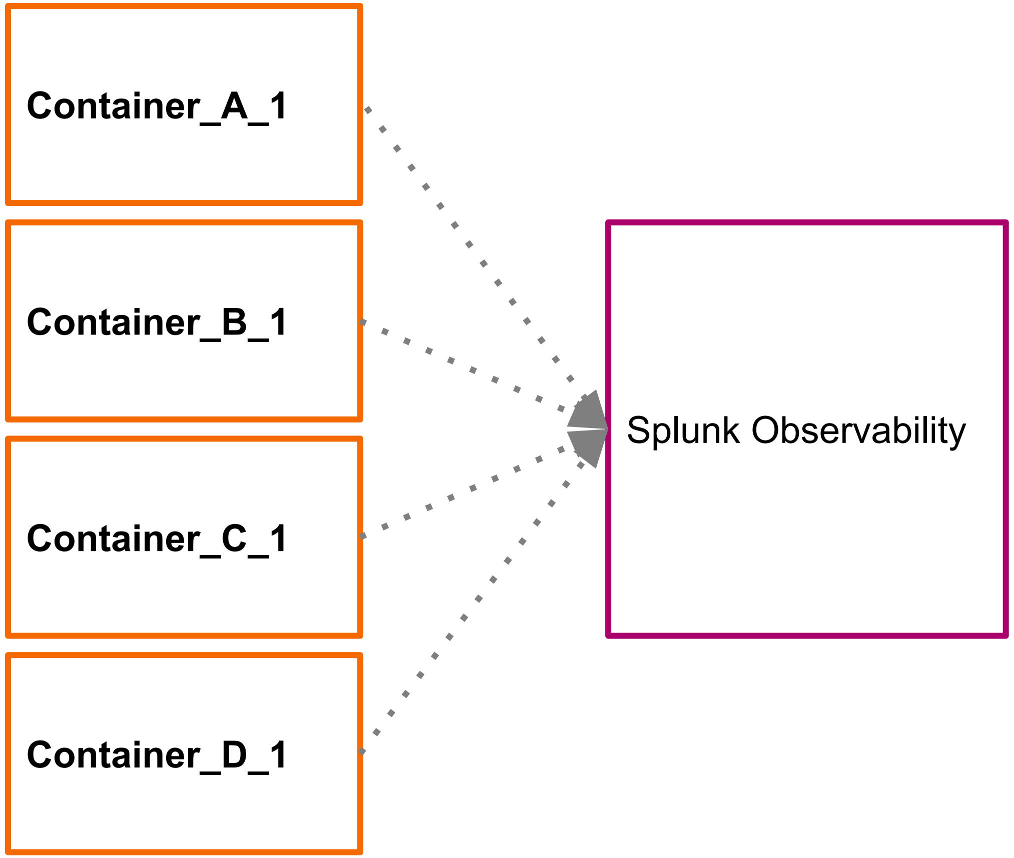
Auto-Clear alerts ?



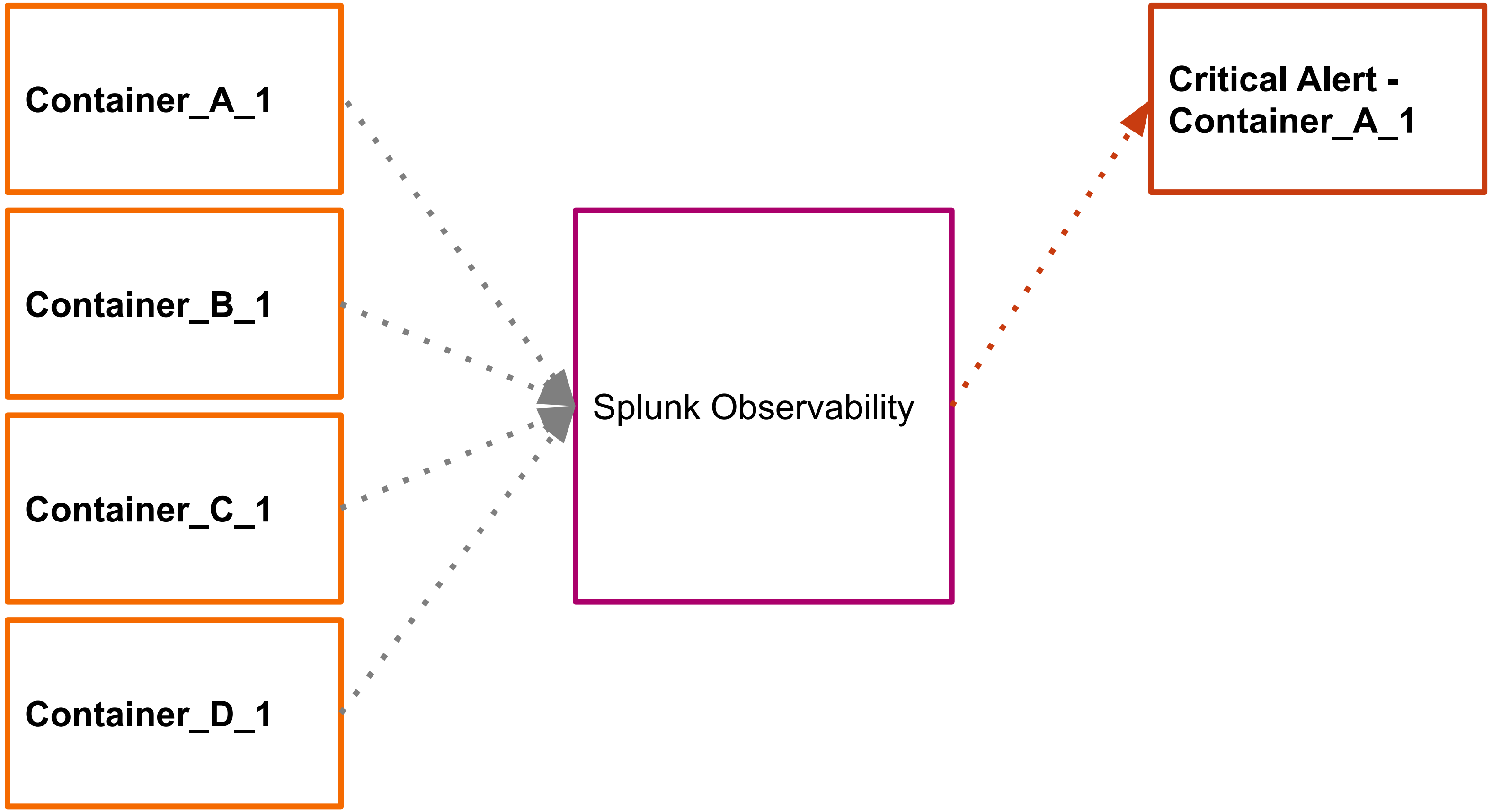
Trigger sensitivity ? percent of duration

Percent of duration ? 100 % of 1h, 4m, etc...

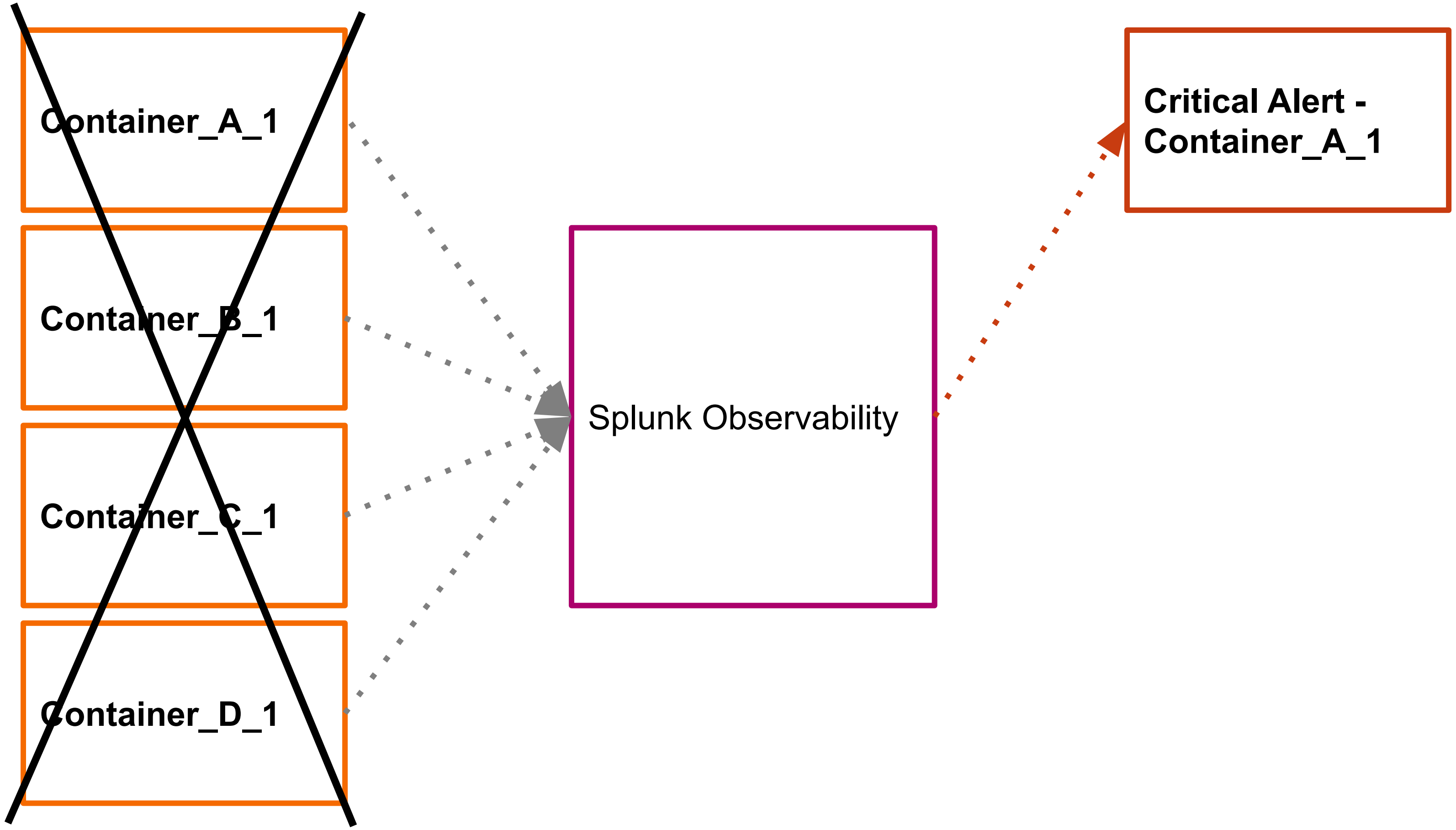
Use AutoClear to prevent ‘Zombie Alerts’



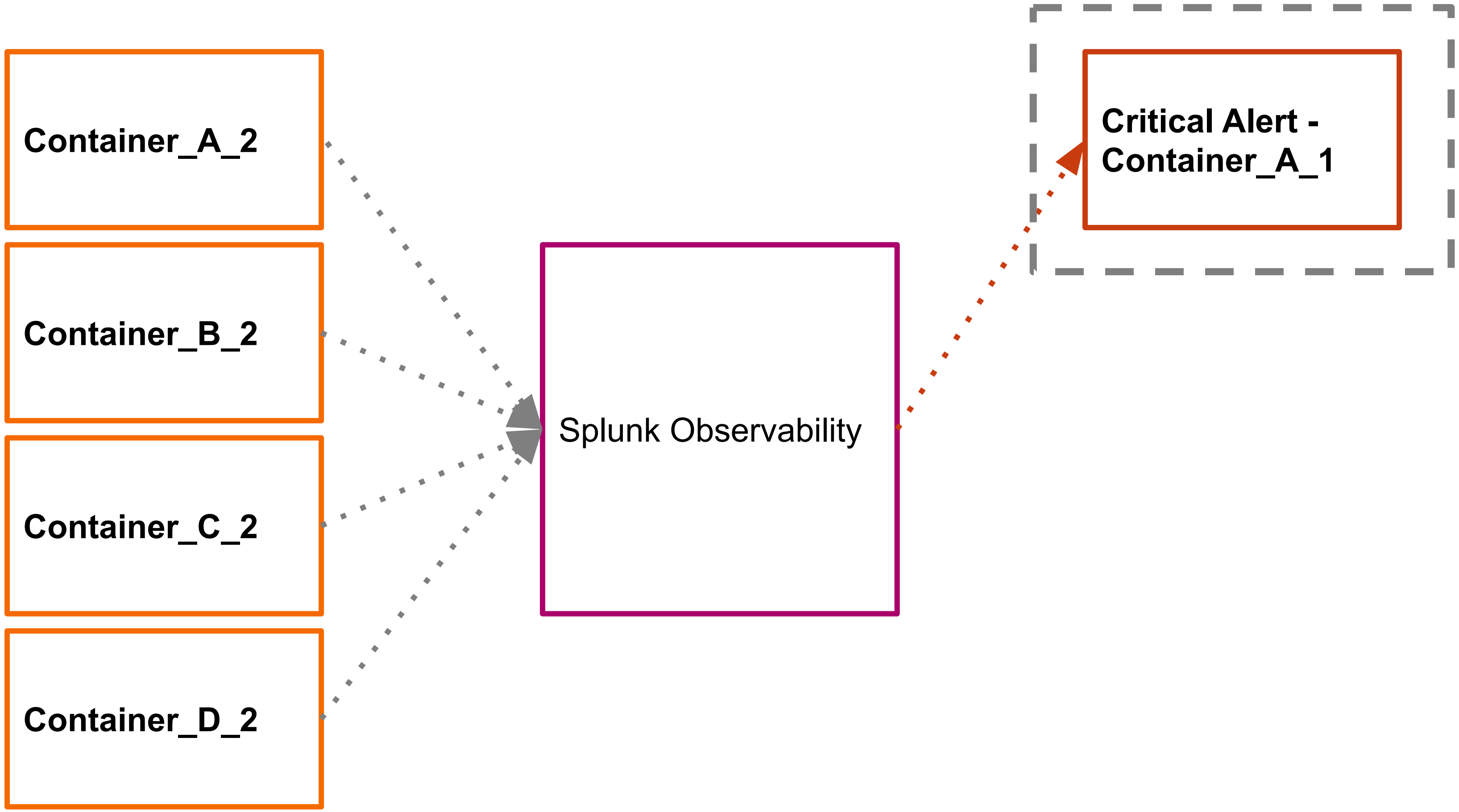
Use AutoClear to prevent ‘Zombie Alerts’



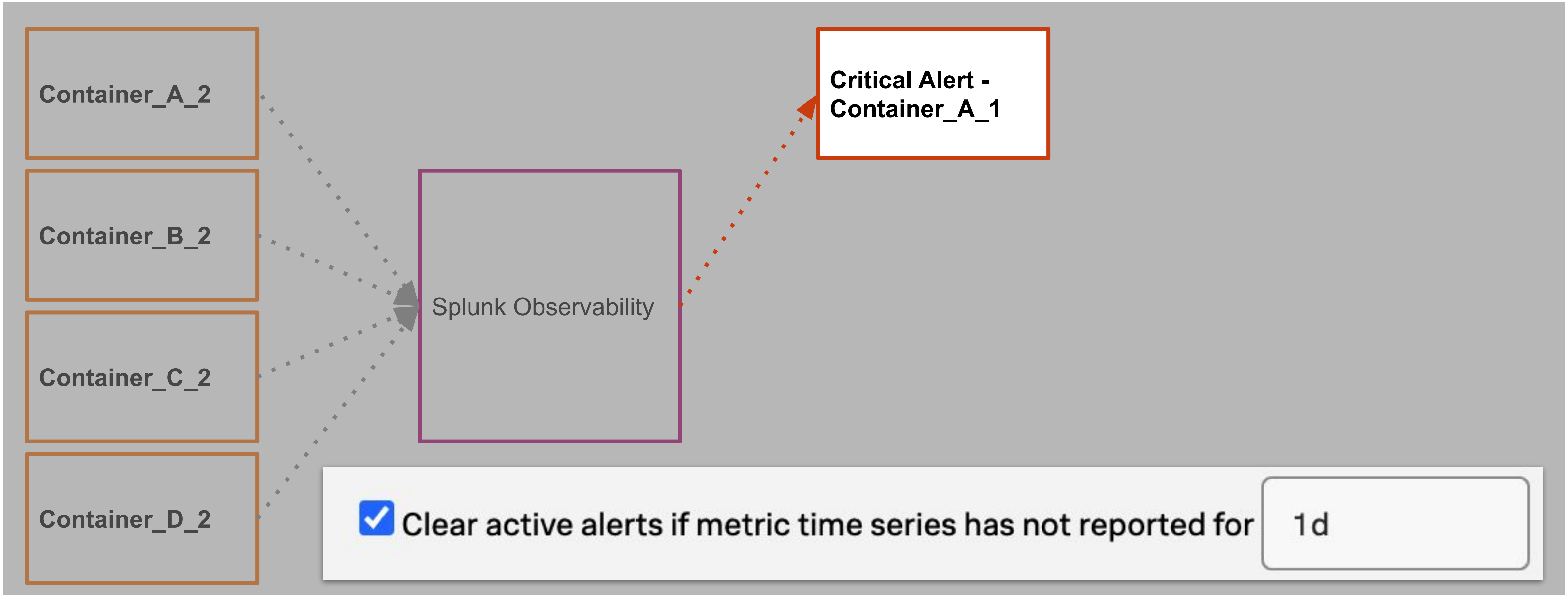
Use AutoClear to prevent ‘Zombie Alerts’



Use AutoClear to prevent ‘Zombie Alerts’



Use AutoClear to prevent ‘Zombie Alerts’



☑ Clear active alerts if metric time series has not reported for 1d

Advanced Options: Clear Conditions

Advanced option available with SignalFlow

Explicitly define desired behavior to clear alerts

Example:

Default - Fire an alert when `CPU > 95` (Alert will clear when `CPU < 95`)

Desired - Fire an alert when `CPU > 95` and **clear the alert when** `CPU < 85`

The Path to be a Detector Jedi Master

1

2

3

Understand the Force

Understand your data (Resolution, Periodicity, Metadata, Aggregation)

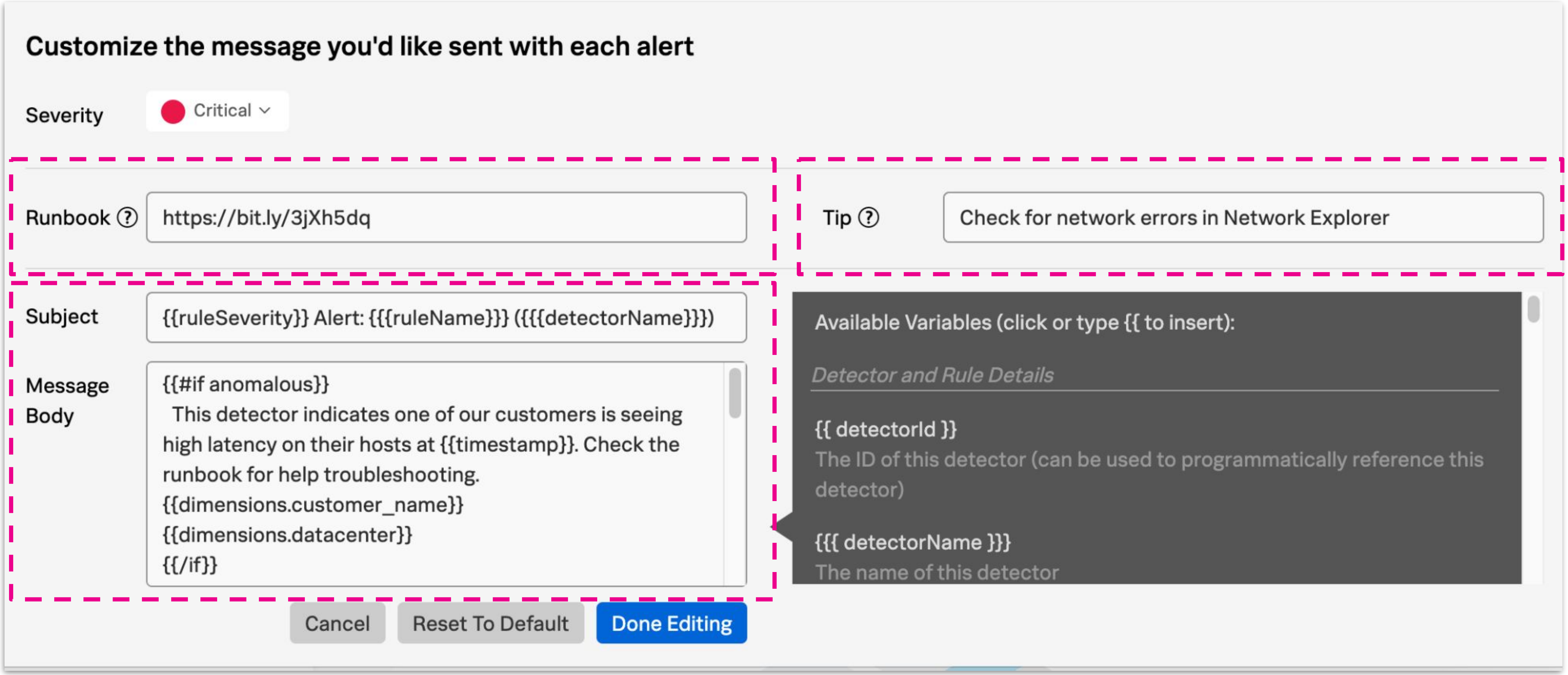
Use all available tools

Use functions available to create the right alerts (Rollup, Alert preview, trigger sensitivity, off conditions)

Assist and train others

Provide context to the alert responder (Tip, Runbook, Aggregation, Message and Title customization)

Giving the alert responder context



Customize the message you'd like sent with each alert

Severity: ● Critical

Runbook: https://bit.ly/3jXh5dq

Tip: Check for network errors in Network Explorer

Subject: {{ruleSeverity}} Alert: {{{ruleName}}} ({{{detectorName}}})

Message Body:

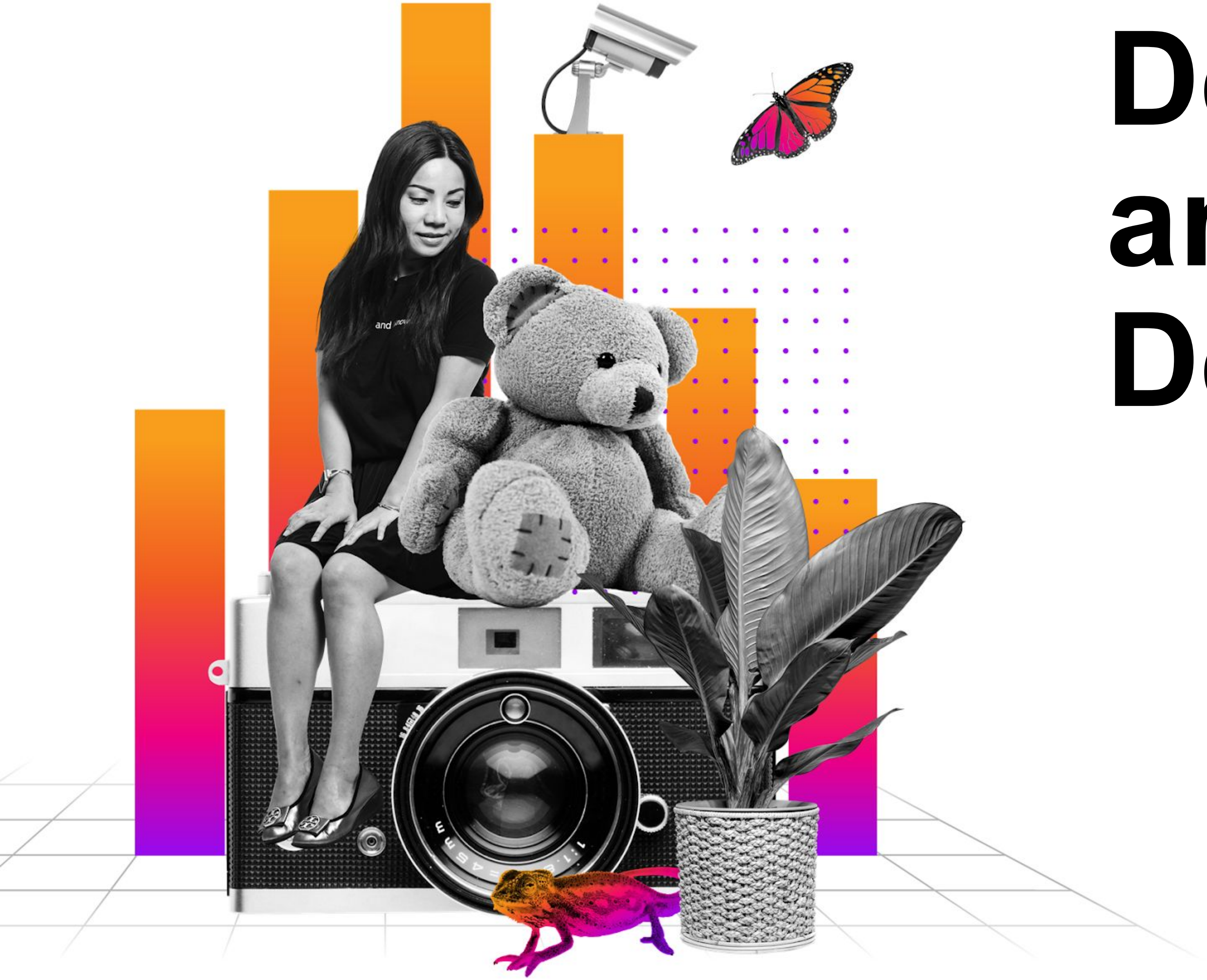
```
{{#if anomalous}}
 This detector indicates one of our customers is seeing high latency on their hosts at {{timestamp}}. Check the runbook for help troubleshooting.
{{dimensions.customer_name}}
{{dimensions.datacenter}}
{{/if}}
```

Available Variables (click or type {{ to insert):

Detector and Rule Details

{{ detectorId }}
The ID of this detector (can be used to programmatically reference this detector)

{{{ detectorName }}}
The name of this detector



Detectors and Alerts Demo

splunk> .conf22

Thank You

splunk> .conf22